19-M-1159

ABS/JN:AE
F.#2017R00031

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH EMAIL ADDRESS: "ELEMER1@MSN.COM" THAT IS STORED AT PREMISES CONTROLLED BY MICROSOFT CORP.	**TO BE FILED UNDER SEAL** APPLICATION FOR SEARCH WARRANT FOR INFORMATION IN POSSESSION OF PROVIDER (EMAIL ACCOUNT) Case No. 19-M-

EASTERN DISTRICT OF NEW YORK, SS:

I, MICHELLE GOLLER, being first duly sworn, hereby depose and state as follows:

I. Introduction

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), duly appointed by law and acting as such.

2. I make this affidavit in support of an application for a search warrant for information associated with the email account "elemer1@msn.com" (the "SUBJECT EMAIL ACCOUNT") that is stored at premises controlled by Microsoft Corp. ("Microsoft"), an email provider headquartered at One Microsoft Way, Redmond, Washington 98052. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I

of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. I have been a Special Agent with the FBI since 2011. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for, among other things, defrauding federal health care programs, including Medicare and Medicaid. These investigations are conducted both in an undercover and overt capacity. I have participated in investigations involving search warrants and arrest warrants. Based on my training and experience, I am also aware that individuals committing fraud commonly use computers and electronic devices in furtherance of their criminal activities including, but not limited to, communications by email. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

4. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: (a) my personal participation in this investigation, (b) reports made to me by other law enforcement authorities, (c) interviews with various individuals, including Medicare beneficiaries, and (d) review of Medicare billing data, emails, bank records and other documents.

5. The FBI and the United States Department of Health and Human Services, Office of the Inspector General ("HHS-OIG") are investigating violations of criminal law by, among others, various health care providers including Elemer Raffai, MD, the user of the SUBJECT EMAIL ACCOUNT; suppliers of durable medical equipment ("DME") and

prescription drugs; purported telemedicine[1] and staffing companies, including Company-1, an entity the name of which is known to me, a Georgia company that purportedly provided medical staffing throughout the United States; and Company-1's owner, Co-conspirator 1 ("CC-1"), an individual whose identity is known to me. As set forth below and based on my training and experience, I submit that there is probable cause to believe that violations of 18 U.S.C. § 287 (false claims); 18 U.S.C. § 1035 (false statements relating to health care matters); 18 U.S.C. § 1341 (mail fraud); 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1347 (health care fraud); 18 U.S.C. § 1349 (conspiracy to commit mail fraud, wire fraud and health care fraud); 42 U.S.C. § 1320a-7b(b)(1) (receiving or soliciting health care kickbacks); 42 U.S.C. § 1320a-7b(b)(2) (offering or paying health care kickbacks); and 18 U.S.C. § 371 (conspiracy to violate 42 U.S.C. §§ 1320a-7b(b)(1) and (b)(2) by offering, paying, soliciting and receiving health care kickbacks) (hereinafter collectively referred to as the "Subject Offenses"), have been committed by Elemer Raffai, Company-1, CC-1, and others known and as yet unknown. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities and fruits of these crimes further described in Attachment B.

6. This affidavit is intended to show only that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter, but simply those facts I believe necessary to establish probable cause to support issuance of the requested warrant. Except where otherwise noted, all conversations and documents described in this affidavit are set forth in part and in substance only.

---

[1] Telemedicine services generally involve connecting medical providers and beneficiaries through real-time, interactive audio and video telecommunications systems to facilitate the providers' provision of medical services to the beneficiaries.

II. Jurisdiction

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

III. Background

A. The Medicare Program

8. The Medicare program ("Medicare") was a federal health care program providing benefits to persons who were at least 65 years old or disabled. Medicare was administered by the Centers for Medicare and Medicaid Services ("CMS"), a federal agency under the United States Department of Health and Human Services. Individuals who received benefits under Medicare were referred to as Medicare "beneficiaries."

9. Medicare was divided into multiple parts. Medicare Part B covered, among other things, costs related to durable medical equipment ("DME"). Generally, Medicare Part B covered these costs only if, among other requirements, they were medically necessary, ordered by a physician and not induced by the payment of kickbacks, bribes or other remuneration.

10. Medicare Part D provided prescription drug coverage to persons who were eligible for Medicare. Medicare beneficiaries obtained Part D benefits in two ways: (a) by joining a Prescription Drug Plan, which covered only prescription drugs, or (b) by joining a Medicare Advantage Plan, which covered both prescription drugs and medical services (collectively, "Part D Plans"). These Part D Plans were operated by private companies, often referred to as drug plan "sponsors," that were approved by Medicare.

11. Medicare and Part D Plans were each a "health care benefit program," as defined by Title 18, United States Code, Section 24(b).

12. In order for DME suppliers and pharmacies (collectively, "Suppliers") to submit claims to Medicare and Part D plans for providing beneficiaries with DME and prescription drugs, those items needed to be prescribed and ordered by a licensed medical provider and needed to be medically necessary, among other requirements.

13. Medicare used the term "ordering/referring" provider to identify the physician who ordered, referred, or certified an item or service reported in that claim. A provider would "order" non-physician items or services for the beneficiary, such as braces, clinical laboratory services, or imaging services.

14. Medicare required ordering/referring physicians to document medical necessity and other coverage for braces. Medicare regulations required health care providers enrolled with Medicare to maintain complete and accurate patient medical records reflecting the medical assessment and diagnoses of their patients, as well as records documenting actual treatment of the patients to whom services were provided and for whom claims for payment were submitted by the physician. Medicare required complete and accurate patient medical records so that Medicare could verify that the services were provided as described on the claim form. These records were required to be sufficient to permit Medicare, through its contractors, to review the appropriateness of Medicare payments made to the health care provider.

15. CMS, through its contractors, issued local coverage determinations, which were determinations by a Medicare Administrative Contractor ("MAC") regarding whether a particular item or service would be eligible for coverage by Medicare as reasonable and necessary. In particular, the MAC that covered New York State, among other locations,

provided in Local Coverage Determination L33318 that as to items for knee orthoses coded L1832, L1833, L1843, L1845, L1850, L1851 and L1852: (1) knee instability had to be documented by examination of the beneficiary and objective description of joint laxity and (2) claims would be denied as not reasonable and necessary when the beneficiary did not meet the above criteria for coverage (e.g., they would be denied if only pain or a subjective description of joint instability was documented).

16. CMS developed the National Plan and Provider Enumeration System ("NPPES") to provide unique identifying numbers for health care providers. When a health care provider registered with NPPES, that provider was given a unique National Provider Identifier ("NPI") number. Information for providers that received NPI numbers was contained in a publicly available database sometimes referred to as the "NPI Registry."

B. Private Insurers

17. Various private entities provided health insurance plans, affecting commerce, under which medical benefits, items and services were provided to individuals, including plans that provided coverage for prescription drugs and DME (the "Private Plans"). Individuals who received benefits under the Private Plans were sometimes referred to as "members" or "beneficiaries."

18. The Private Plans were each a "health care benefit program," as defined by Title 18, United States Code, Section 24(b).

19. As with Medicare and Part D Plans, Private Plans generally required a licensed medical provider to prescribe or order drugs and DME, and required that the items be medically necessary in order to pay the Supplier, directly or indirectly, for reimbursement for DME and drugs.

C. The Anti-Kickback Statute

20. The Anti-Kickback Statute, Title 42, United States Code, Section 1320a-7b(b)(1), provides in relevant part:

> Whoever knowingly and willfully solicits or receives any remuneration (including any kickback, bribe, or rebate) directly or indirectly, overtly or covertly, in cash or in kind—
>
> (A) in return for referring an individual to a person for the furnishing or arranging for the furnishing of any item or service for which payment may be made in whole or in part under a Federal health care program, or
>
> (B) in return for purchasing, leasing, ordering, or arranging for or recommending purchasing, leasing, or ordering any good, facility, service, or item for which payment may be made in whole or in part under a Federal health care program,

shall be guilty of a felony.

21. Medicare and Part D Plans were each a "Federal health care program," as defined by Title 42, United States Code, Section 1320a-7b(f).

D. Elemer Raffai

22. Elemer Raffai was a resident of Malone, New York who worked as a physician and was licensed to practice medicine in New York. In addition, Raffai was enrolled in the Medicare program beginning in approximately February 2011. Raffai was also registered with NPPES, which listed his primary specialty as orthopaedic surgery.

23. On or about June 22, 2017, Elemer Raffai's enrollment in the Medicare program was revoked for, among other reasons, failure to document or provide CMS access to documentation, along with a one year bar for enrolling in the Medicare program again. Specifically, on or about March 31, 2017 CMS requested medical records for 25 beneficiaries for

whom Elemer Raffai was the ordering provider for DME, but Raffai did not provide the requested records to CMS.

E. Company-1 and CC-1

24. Company-1 was an entity located in Alpharetta, Georgia, that paid providers for their purported provision of telemedicine services to beneficiaries who were enrolled in Medicare, Part D Plans and Private Plans.

25. CC-1 was an owner and operator of Company-1.

IV. Probable Cause

26. The facts set forth below establish probable cause to believe that, from at least June 2016 to June 2019, in the Eastern District of New York and elsewhere, Elemer Raffai, Company-1, CC-1 and others engaged in violations of the Subject Offenses.

A. Overview of the Illegal Kickback Scheme

27. As discussed in more detail below, the scheme that is the subject of this investigation involves Company-1, a company that contracted with various physicians and made this network of physicians available to Company-1's clients, including other telemedicine companies, pharmacies and companies that provided DME[2] and prescription drugs (collectively, the "Clients"). The evidence learned to date shows that the Clients paid kickbacks to get prescriptions from physicians for the purpose of submitting false and fraudulent claims to Medicare or to private insurance companies for reimbursement under the purported provision of telemedicine services.

[2] DME can include, for example, knee braces, hospital beds, walkers and wheelchairs.

28. The scheme generally appears to proceed as follows: (a) a Client provided one of Company-1's physicians with order forms and information for a Medicare or private insurance beneficiary and sometimes connected one of Company-1's physicians with the beneficiary by telephone; (b) the physician wrote a prescription for DME or medication, which was medically unnecessary, as described below, but was necessary for the item to be reimbursed; (c) the Client paid Company-1 a kickback in return for the prescription; (d) Company-1 in turn paid the physician a portion of the kickback/bribe it received from the corrupt supplier; and (e) as a result of the physician's prescription, a Supplier sent the DME or prescription drug to the beneficiary, submitted the related claim(s) for reimbursement to Medicare or a private insurance company and made a profit.

29. As described in more detail below, between approximately June 2016 and June 2019, Elemer Raffai purported to practice telemedicine while participating in this scheme by signing medically unnecessary prescriptions and orders for items covered by Medicare and private insurers, without conducting an examination, and in return for bribes and kickbacks.

B. The Role of CC-1 and Company-1 in the Illegal Kickback Scheme

30. On February 17, 2016, HHS-OIG agents interviewed CC-1 and confirmed his/her email address (the "CC-1 Email Address"), which is known to me. CC-1 also confirmed that s/he was the owner of Company-1 and stated that the company provided medical staffing throughout the United States.

31. During the February 17, 2016 interview, CC-1 further stated that approximately two years earlier, s/he started a telemedicine arrangement with physicians and the Clients (which he acknowledged included pharmacies and DME suppliers), who paid Company-1 for the physicians' services. CC-1 additionally stated that the physicians consulted with

patients who were interested in obtaining body braces, pain creams, and other items and services. CC-1 represented that Company-1 paid the Company-1-affiliated physicians an amount, such as $30 for each consult. CC-1 admitted that the Clients paid Company-1 for the prescriptions the physicians wrote—$39 for a back brace prescription, for example. CC-1 further admitted that the objective of the consults was for the physicians to write prescriptions for the Clients.[3]

32. During the February 17, 2016 interview, CC-1 agreed to provide the agents conducting the interview with a list of Clients, and shortly thereafter emailed one of the agents a document named "Client List" from the CC-1 Email Address.

C. Emails Showing Relationship Between Company-1 and Elemer Raffai

33. During the course of a related investigation conducted by FBI and HHS-OIG, agents obtained emails pursuant to a search warrant for the CC-1 Email Address. I have reviewed certain emails obtained pursuant to that search warrant, which include email communications between CC-1 and Elemer Raffai and between CC-1 and some of Company-1's Clients (the "CC-1 Emails").

34. The CC-1 Emails I have reviewed indicate that Elemer Raffai used the SUBJECT EMAIL ACCOUNT to communicate with CC-1 and in connection with the purported practice of telemedicine. For example:

---

[3] CC-1 contended that s/he was aware of situations where a patient refused to speak with the physician, and in those instances the physician was still entitled to be paid for the contact with the patient (even though no consult actually occurred). Based on the evidence developed in this investigation, and my experience as a Special Agent, and the inconsistencies in CC-1's various statements, it is clear Clients were not merely paying for purported medical consults, but were paying Company-1 kickbacks for prescriptions.

a. Elemer Raffai contacted CC-1 via LinkedIn on or about June 17, 2017, stating that he was "searching for a telemedicine job opportunity." A few days later, CC-1 sent an email to the SUBJECT EMAIL ACCOUNT describing the telemedicine opportunities that were available, including non-narcotic pain creams, DME braces, lab tests and cancer screens.

b. On July 13, 2017, Elemer Raffai sent an email from the SUBJECT EMAIL ACCOUNT to CC-1 stating, "Someone from, I believe, [Company-2] just called me. He says he can get me a job doing our insurance patients are [sic] in New York State. As you know my Pecos is temporarily inactive so I can't do Medicare. Can you send me a link to their EMR and help me set up. The gentleman said he would send me an email but I haven't received it yet."[4] CC-1 responded "You will have to tell him that…we are staying away from Medicare patients." (ellipsis in original).

D. Emails Showing Corrupt Relationship Between Company-1 and Its Clients

35. The CC-1 Emails I have reviewed also indicate that Elemer Raffai and other physicians affiliated with Company-1 were paid for writing prescriptions, not for their time or services.

36. For example, in an email dated April 4, 2018, a person writing on behalf of Company-3, an entity the identity of which is known to me, sent an e-mail to CC-1 and others, attaching multiple documents described as "invoices and doctor totals for this pay period." One of the attached documents was a spreadsheet that listed more than 100 doctors' names, and

[4] The reference to "Pecos" appears to be a reference to the Medicare Provider Enrollment, Chain and Ownership System, commonly referred to as "PECOS," an online provider and supplier enrollment system.

provided information in three corresponding columns: "Scripts," "Non payable" and "Consults." The "Consults" column was simply the formula of "Scripts" minus "Non payable." The number of "Scripts" was almost always the same as the number of "Consults," because the "Non payable" value was almost always zero. For example, in one spreadsheet, Elemer Raffai was identified as having three "Scripts" and three "Consults." Another document attached to the April 4, 2018 email was an invoice for 731 "Consults" over a two-week period, for $32,895.00 (which equals $45 for each "consult"). Based on my knowledge and experience, the above email indicates that this Client was tracking the number of "scripts" (i.e., prescriptions) in connection with payments to Company-1, suggesting the payments were tied to the prescriptions.

E. Beneficiaries

37. Based on interviews of Medicare beneficiaries, Elemer Raffai prescribed and ordered DME that supported false and fraudulent claims to Medicare because, among other things, the items were ordered without an appropriate examination of the beneficiary. In particular, as described above (see ¶ 15), LCD L33318 required, among other things, documented examination of the beneficiary for knee braces code L1832, L1833, L1843, L1845, L1850, L1851 and L1852 to be covered by Medicare.

38. According to Medicare claims data, on or about March 8, 2017, approximately $4,015 in claims were submitted on behalf of Beneficiary-1, a Medicare beneficiary who resided in Clifton Park, New York, for certain DME, including a knee brace (code L1833), as well as a back brace and wrist-hand brace. The claims data identified Elemer Raffai as the referring provider (i.e., the prescriber).

39. Another law enforcement agent and I interviewed Beneficiary-1 on or about September 13, 2017. Beneficiary-1 informed us that s/he received a hand, back and knee

brace in the mail and that s/he understood the braces came from Medicare. Beneficiary-1 further reported that s/he had no idea who Elemer Raffai was, and s/he did not speak to a doctor or nurse on the phone prior to receiving the braces.

40. According to Medicare claims data, on or about March 30, 2017, approximately $3,713 in claims were submitted on behalf of Beneficiary-2, a Medicare beneficiary who resided in Ballston Spa, New York, for certain DME, including a knee brace (code L1833), as well as a back brace and should-elbow-wrist-hand brace. The claims data identified Elemer Raffai as the referring provider.

41. Another law enforcement agent and I interviewed Beneficiary-2 on or about September 13, 2017. Beneficiary-2 informed us that s/he received a telephone call from a medical supply company that told him/her s/he could receive free braces. Beneficiary-2 further informed us that s/he had never heard of Elemer Raffai and the braces were still in their packages from when s/he received them months earlier.

42. According to Medicare claims data, on or about and between August 25, 2016 and August 30, 2016, approximately $3,224 in claims were submitted on behalf of Beneficiary-3, a Medicare beneficiary who resided in Brooklyn, New York, for certain DME, including a knee brace (code L1833), as well as a back brace, suspension sleeve and wrist brace. The claims data identified Elemer Raffai as the referring provider.

43. On or about November 7, 2019, HHS-OIG agents interviewed Beneficiary-3. Beneficiary-3 informed the HHS-OIG agents that s/he received phone calls offering orthotic braces such as elbow, back, neck, ankle and knee braces. Beneficiary-3 informed the HHS-OIG agents that s/he recalled speaking to a doctor on the phone who said something to the effect of, "I'm a doctor, I see you need all this," and Beneficiary-3 did not

recall the doctor's name, nor did s/he recall a Dr. Elemer Raffai. Beneficiary-3 further informed the HHS-OIG agents that s/he received a back brace and knee brace in the mail and wore some of them for a little while, but s/he did not receive a knee suspension sleeve or a right wrist brace, and instead s/he eventually purchased a wrist brace on his/her own because it did not arrive.

44. According to Medicare claims data, on or about December 6, 2016, approximately $3,800 in claims were submitted on behalf of Beneficiary-4, a Medicare beneficiary who resided in Brooklyn, New York, for certain DME, including a knee brace (code L1833), as well as a back brace, suspension sleeve, and wrist-hand brace. The claims data identified Elemer Raffai as the referring provider.

45. On or about November 7, 2019, HHS-OIG agents interviewed Beneficiary-4. Beneficiary-4 informed the HHS-OIG agents that s/he received wrist, knee and back braces in the mail, but did not request the braces; although Beneficiary-4 attempted to use the braces after they arrived, s/he found them too complicated. Beneficiary-4 further informed the HHS-OIG agents that s/he did not speak to a doctor over the phone regarding orthotic braces and did not know Elemer Raffai

46. According to Medicare claims data, on or about May 30, 2017, approximately $3,109 in claims were submitted on behalf of Beneficiary-5, a Medicare beneficiary who resided in Brooklyn, New York, for certain DME, including a back brace, shoulder-elbow-wrist-hand brace (right side) and wrist-hand brace (left side). The claims data identified Elemer Raffai as the referring provider.

47. On or about November 8, 2019, HHS-OIG agents interviewed Beneficiary-5. Beneficiary-5 informed the HHS-OIG agents that s/he spoke on the phone with a doctor for approximately one to two minutes and only discussed a back brace with the doctor.

Beneficiary-5 could not recall the name of the doctor, but told the HHS-OIG agents that s/he had never heard of Elemer Raffai. Beneficiary-5 further informed the HHS-OIG agents that s/he never received a shoulder brace or wrist brace in the mail, but did receive a back brace in the mail; Beneficiary-5 could not use the back brace because it was too heavy, and s/he eventually request a lighter brace for which s/he paid approximately $150 out of pocket because s/he was told Medicare would only pay for the brace once every five years.

48. I have also reviewed additional Medicare claims data where Elemer Raffai is listed as the referring provider for DME. Based on my review of this data, between approximately January 2017 and November 2018, suppliers submitted approximately $5.4 million in claims for DME where Elemer Raffai was the prescribing physician, and Medicare paid approximately $2.3 million on those claims, including several claims on behalf of multiple beneficiaries with addresses within the Eastern District of New York.

49. In addition, I have reviewed claims data and other documents from private insurers identifying Elemer Raffai as the referring provider for expensive prescription drugs between at least approximately October 2017 and June 2019, including several claims involving, among others, Pharmacy-1, an entity the identity of which is known to me, which was located within the Eastern District of New York.

F. Interviews of Elemer Raffai

50. On June 23, 2017, an agent with HHS-OIG telephonically interviewed Elemer Raffai. During this interview, Raffai provided the following information, in substance and in part:

a. Raffai had a contract with a California company, Company-4, an entity the name of which is known to me, which paid him $20 for each telephonic sales

consultation where he would call patients to prescribe them medical equipment. Each day, Raffai received from Company-4 a list of approximately 25 to 30 names with a telephone number for each individual.

b. Raffai claimed that he called the patients to assess their needs for medical equipment, and he prescribed braces for approximately seven to nine patients per day. Raffai was paid for each patient he prescribed.

51. On September 22, 2017, another agent and I interviewed Elemer Raffai in person. During this interview, Raffai provided the following information, in substance and in part:

a. Raffai had been practicing telemedicine from his home since approximately May 2016, when he was injured while working. Raffai worked for a number of telemedicine companies during this time, and typically signed a contract with the company where the company agreed to pay him between $20 to $30 for each telephonic medical consultation he made. Raffai was generally paid by direct deposit.

b. Raffai claimed that he would get paid whether or not he agreed to write prescriptions and that he was not pressured to complete consultations or write prescriptions he did not believe were medically necessary.

c. Raffai acknowledged that he did not conduct a physical exam, and instead reviewed the patient's electronic medical records and asked the patients what he characterized as standard medical questions, such as "where is the pain?" Raffai further acknowledged that because there was no physical exam, he simply believed what the patient told him.

d. Raffai understood the medical records were created by nurses at the telemedicine companies, but he did not know if the nurses were from the United States.

52. In October 2017, HHS-OIG requested that Elemer Raffai provide copies of employment contracts he entered into with respect to telemedicine companies and copies of 21 specified patient files. The patient files included documents reflecting that they had been sent to the SUBJECT EMAIL ACCOUNT, as the documents contained references that they were "emailed to Elemer Raffai MD [] (elemer1@msn.com) for signature," and that the signed documents were "emailed to Elemer Raffai MD [] (elemer1@msn.com)." These patient files included orders for DME for Medicare beneficiaries with addresses in Brooklyn, Westbury and Valley Stream, New York and other locations.

53. On January 31, 2018, an HHS-OIG Special Agent emailed the SUBJECT EMAIL ACCOUNT to ask whether Elemer Raffai was using a business address on Broadway in New York City. Raffai replied that he was not, that his business address was in Malone, New York, and he further commented that: "[O]ne of my Telemedicine companies has a pharmacy on Broadway that they use for prescriptions of pain creams and anti acid reflux meds. And I noticed that they put my name as the prescriber above that address." Raffai later explained the telemedicine company he was referring to was his "main company affiliation called [Company-4]. Their main office is in Beverly Hills, CA." The HHS-OIG Special Agent then asked whether the New York City address was for Company-4, and Raffai replied that he did not know "if they have an office at that New York City address, But [sic] it's the address that appears on the script underneath my name. So actually I really don't know what that address is for."

54. I have reviewed a report prepared by the special investigations unit of Fidelis, a private insurer that provides its members with coverage for health care benefits items

and services under Medicare Advantage, Part D and Medicaid Managed Care plans as well as Private Plans. According to that report, on or about January 30, 2019, Fidelis investigators interviewed Elemer Raffai, during which interview, Raffai informed the investigators, in substance and in part, that he did telemedicine work from his home for two telemedicine companies, and was reimbursed $20 per consultation. According to Raffai, he had a list of prescriptions he was allowed to prescribe for patients from the telemedicine company. Raffai acknowledged that in his own medical practice, he was not restricted to a list of medications to prescribe.

G. Letter from Elemer Raffai

55. On or about August 7, 2017, following a phone call between Elemer Raffai and the New York State Office of Professional Medical Conduct ("OPMC"), Raffai submitted a letter to OPMC, in which Raffai discussed, among other things, the telemedicine companies he worked for. Specifically, Raffai provided OPMC with the names of various companies, contact persons, phone numbers and emails, including, among others, CC-1 and Company-1. In addition, on or about June 6, 2017, Raffai submitted to the OPMC physician monitoring program a data sheet that listed his email address as the SUBJECT EMAIL ACCOUNT.

V. Background Concerning Email

56. In my training and experience, I have learned that Microsoft provides a variety of on-line services, including email access, to the public. Microsoft allows subscribers to obtain email accounts at the domain name "msn.com," like the SUBJECT EMAIL ACCOUNT. Subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of

Microsoft are likely to contain stored electronic communications (including retrieved and unretrieved email for Microsoft subscribers) and information concerning subscribers and their use of Microsoft's services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

57. In general, an email that is sent to a Microsoft subscriber is stored in the subscriber's "mail box" on Microsoft's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Microsoft's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Microsoft's servers for a certain period of time.

58. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information nonetheless often provides clues to their identity, location or illicit activities.

59. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records

of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

60. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

61. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling investigators to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email

communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

VI. Special Instructions Regarding Review of the Seized Material

62. With respect to law enforcement's review of the seized material identified in Attachment B, law enforcement (i.e., the federal agents and prosecutors working on this investigation and prosecution), along with other government officials and contractors whom law enforcement deems necessary to assist in the review of the seized material (collectively, the "Review Team") shall review, in the first instance, the seized material.

63. If, during the review of the seized material, the Review Team finds potentially privileged materials, the Review Team will: (1) immediately cease its review of the potentially privileged materials at issue; (2) segregate the potentially privileged materials at issue; and (3) take appropriate steps to safeguard the potentially privileged materials at issue. Nothing in this Affidavit shall be construed to require the Review Team to cease or suspend review of all the seized material upon discovery of the existence of potentially privileged materials within a portion of the seized material.

VII. Conclusion

64. In sum, there is probable cause to believe that the SUBJECT EMAIL ACCOUNT contains evidence of the Subject Offenses.

65. Based on the forgoing, I request that the Court issue the proposed search warrant. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Microsoft. Because the warrant will be served on Microsoft, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

66. Furthermore, I respectfully request that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing these documents is necessary because the items and information to be seized are relevant to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Based upon my training and experience, I have learned that participants in fraudulent schemes often actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other

participants in the scheme as they deem appropriate. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation. Some of the evidence in this investigation involves communications that can be transferred to alternate platforms (including encrypted platforms and platforms beyond the jurisdictional reach of U.S. legal process). If alerted to the existence of the warrant, there is reason to believe that the subjects under investigation will destroy that evidence and change their patterns of behavior.

67. Pursuant to 18 U.S.C. § 2705(b) and for the reasons stated above, it is further requested that the Court issue an Order commanding Microsoft not to notify any person (including subscribers or customers of the account(s) listed in the attached warrant) of the existence of the attached warrant for the period of one year from the date of the Order, except

that Microsoft may disclose the warrant to its respective attorney for the purpose of receiving legal advice.

Respectfully submitted,

Michelle Goller
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on December 12, 2019

HONORABLE ROBERT M. LEVY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

This warrant applies to information associated with the email address:

(1) "elemer1@msn.com";

that is stored at premises controlled by Microsoft Corp., a company that accepts service of legal process at One Microsoft Way, Redmond, Washington 98052.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Microsoft Corp. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails from June 1, 2016 to the present associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken. The Provider is hereby ordered to disclose the information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of false claims, in violation of Title 18, United States Code, Section 287; false statements relating to health care matters, in violation of Title 18, United States Code, Section 1035; mail fraud, in violation of 18, United States Code, Section 1341; wire fraud, in violation of Title 18, United States Code Section 1343; health care fraud, in violation of Title 18, United States Code, Section 1347; conspiracy to commit wire fraud and health care fraud, in violation of Title 18, United States Code, Section 1349; receiving or soliciting health care kickbacks, in violation of Title 42, United States Code, Section 1320a-7b(b)(1); offering or paying health care kickbacks, in violation of Title 42, United States Code, Section 1320a-7b(b)(2); and conspiracy to violate 42 U.S.C. §§ 1320a-7b(b)(1) and (b)(2) by offering, paying, soliciting, and receiving health care kickbacks, in violation of 18 U.S.C. § 371, between June 1, 2016 and the present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. A fraudulent scheme or conspiracy involving the submission of claims to Medicare or any other health insurance provider for prescription drugs and durable medical equipment;

b. A scheme or conspiracy involving the solicitation and payment of illegal kickbacks in connection with the provision of durable medical equipment

and prescription drugs under a Federal health care program, including Medicare;

c. Records and communications relating to patient files, bills, invoices, and claims for payment/reimbursement for services or equipment billed, provided, or alleged to have been provided to patients relating to the provision of telemedicine services, durable medical equipment or prescription drugs, including but not limited to, reimbursement claim forms, explanations of medical benefits, dispensing orders, detailed written orders or prescriptions, certificates of medical necessity, information from physician(s) concerning the patients' diagnosis, and proof of delivery of services and/or items and/or equipment that were submitted to Medicare or any other health insurance provider;

d. Records and communications relating to the provision of telemedicine services, including financial transactions related to the provision of telemedicine services;

e. Records and communications relating to the provision of durable medical equipment or prescription drugs, including records regarding prescriptions for durable medical equipment or prescription drugs;

f. Records and communications relating to notice of overpayment and request for refunds from Medicare or any other health insurance provider;

g. Records and communications relating to patients who were prescribed durable medical equipment or drugs;

h. Records and communications relating to companies that supply durable medical equipment or prescription drugs;

i. Evidence indicating the email account owner's state of mind as it relates to the crimes under investigation;

j. Records relating to who created, used, or communicated with the account or identifiers, including records about their identities and whereabouts.

III. Treatment of Potentially Privileged Information

With respect to law enforcement's review of the materials seized pursuant to this search warrant (the "Materials"), law enforcement (i.e., the federal agents and prosecutors working on this investigation and prosecution), along with other government officials and

contractors whom law enforcement deems necessary to assist in the review of the Information (collectively, the "Review Team") shall review, in the first instance, the Materials.

If law enforcement determines that all, some or a portion of the Materials constitutes or may contain material subject to a claim of attorney-client privilege or work-product protection (the "Potentially Privileged Materials"), the Review Team will: (1) immediately cease its review of the specific Potentially Privileged Materials at issue; (2) segregate the specific Potentially Privileged Materials at issue; and (3) take appropriate steps to safeguard the specific Potentially Privileged Materials at issue.

Nothing in this Attachment B.III shall be construed to require law enforcement to cease or suspend the Review Team's review of the Materials upon discovery of the existence of Potentially Privileged Materials within the Materials.